SCP PERSONAL INFORMATION PROTECTION CODE

Table of Contents

1. Management 1

2. Notice 1

3. Providing Choice and Obtaining Consent 2

4. Collection 2

5. Use and Retention 3

6. Disposal Issues 3

7. Access 3

8. Disclosure to Third Parties 4

9. Security 4

10. Quality 4

11. Monitoring and Enforcement 5

12. Information not to be made available 5

1. Management

Senior Concierge Providers policy is to:

- Create a full-time privacy officer reporting directly to the chief operating officer;
- Create compliance teams that report to the privacy officer as the focus of responsibility for privacy issues, including a representative from each business unit that has a substantial interest in the collection, use, retention and disclosure of personal information; and
- Create a working committee that meets regularly to coordinate the efforts of the team members.

It is recommended that the chief financial officer, the marketing director, the sales manager and the internal auditor should not be selected as the privacy officer of the corporation or as members of the privacy compliance team, since the holders of these offices may have a role in developing the organization's privacy code and a perceived conflict of interest may result where compliance with the code is challenged. The same may be said of the general counsel, although more latitude is generally given to that office.

2. Notice

Senior Concierge Providers policy is that the purpose for collecting personal information be specifically and clearly stated in concrete terms; this means that the organization should itemize the marketing uses to be made of the information collected rather than using the umbrella phrase "marketing purposes" or the like.

An adequate definition of purposes should satisfy the following criteria:

- Clearly specify the purposes for the collection of the information and explain why that information is required;
- Establish a specific time frame for information collection, use and retention;
- Explain purposes in layman's terms and explain any abbreviations;
- Provide sufficient information to allow the individual to make a meaningful choice about whether they want to provide personal information for the organization ' s stated purposes;
- Communicate the purposes for collecting the personal information to the individual at or before the time of collection; and
- Document the purposes for collecting the information and make it available to employees collecting the information as a reference for use when individuals challenge the collection of particular information.

Senior Concierge Providers policy is that a privacy brochure or flyer would include the identity and contact information for the organization's privacy officer and clearly explain that:

- The organization does not collect any more information than is necessary to deliver its goods and services;

- The organization only collects personal information with the knowledge and consent of the individual, except in very limited and specific circumstances permitted by law;

- The organization limits the uses of this information, limits its retention, ensures its accuracy to the best of its ability where the information will be used for decision-making, and protects the information against unauthorized access or use;

- (if applicable), the organization intends to disclose the information to third parties, the identity of the third parties, as well as the individuals options to withdraw consent for such disclosures or for any options uses; and

- Individuals have access to their personal information upon request, and how to make such a request.

3. Providing Choice and Obtaining Consent

Senior Concierge Providers policy is that express (as opposed to imply) consent is preferred, particularly in respect of sensitive information, such as medical and financial information and information about education or employment. Express consent might be obtained:

- Via telephone or in person: For example: “Would you like us to send you more information by mail or may we call you in the future to discuss our services?” (wait for yes or no response);

- Via a response card: For example: “ Please check the box if you would like to receive further information about our services ” (affirmative action required to initiate further contact);

- Via a telephone key pad, computer or other electronic means: For example: “ Press the following key if you wish to have your name included on our mailing list ” ;

- Through a signature: For example: “Your signature is required to authorize the above application form. Information provided will only be use for the purposes specified. ”

When obtaining personal information from another organization, one should ensure that this disclosure of personal information is within the scope of the consent provided to the original collector of that information. Further, consent should be provided willingly; there should be no link between the provision of the services in question and the supply of the requested personal information, unless the provision of the services clearly requires this information, such as financial information for the purpose of issuing credit.

4. Collection

Senior Concierge Providers policy is that information should not be collected

surreptitiously and information should not be gathered from other people such as family members or colleagues or acquaintances without the knowledge and consent of the individual. Social insurance numbers or health card numbers should not be collected unless a special need exists.

5. Use and Retention

Senior Concierge Providers policy is that any use or retention of personal information collected by the organization be within the scope of the consent obtained. Information collected should be destroyed or rendered anonymous once it is no longer needed for the purpose for which it was collected.

A retention policy should be based on how long the information is required:

- To fulfill the fundamental purposes for which it is collected and any secondary purposes to which the individual has consented;
- To allow the individual to verify the accuracy or completeness of the information and have the information corrected or updated, if necessary, in the event of a query or a dispute; and
- To be held to meet customer expectations, established industry norms, standard accounting procedures and regulatory and legal requirements.

6. Disposal Issues

When disposing of computers, diskettes, magnetic tapes, hard-drives and any other magnetic media that contain personal information, all data must be erased and/or the hardware must be destroyed. When disposing of waste and recycling paper, all documents containing personal information should be placed in secure, locked containers until they are shredded.

7. Access

Senior Concierge Providers policy is the following procedures:

- A timely response from the organization, either providing the information requested or written reasons why that information cannot be provided. If a specific exemption is relied upon, it should be cited. The individual should also be advised of any redress procedures if information has been withheld.
- The individual should be given an opportunity to challenge the accuracy of any information in the file. This might be accomplished by including a form along with the requested information, which asks the individual to detail any perceived discrepancies.
- Information files should be maintained in a way that facilitates efficient access by the individual at reasonable or no cost. They should also give a good overview of what information is maintained, its source and how it is used.
- Reasonable procedures must be in place to verify the identity of the individual making the request for information.

8. Disclosure to Third Parties

Where the organization discloses personal information to a third party, the organization should communicate any maximum retention times to that third party. Further, the third party using the information should be contractually obligated to return or destroy it after the specified use is complete.

9. Security

Senior Concierge Providers policy is that the following precautions be taken when collecting personal information:

- Staff should be specifically assigned to data security. Further, staff members should participate in regular training programs to keep abreast of technical and legal issues.
- Physical access to computer operations and paper or micrographic files that contain personal information should be restricted.
- Sensitive files should be segregated in secure areas or computer systems made available only to qualified persons.
- Audit procedures and strict penalties should be in place to prevent telephone fraud and theft of equipment and information
- All employees should be required to follow strict password and password protection procedures; further, employees should be required to change their passwords and to avoid using the more obvious password creation methods.
- Encryption should be used to protect extremely sensitive information.
- Computer systems should be regularly tested for vulnerability to hackers.
- Employees should be trained never to leave computer terminals unattended when personal information is on the screen.
- When providing copies of information to others, employees should ensure that non-essential information is removed and that personal information that has no relevance to the transaction is either removed or masked.
- All employees who handle personal information should be trained to recognize “pretext” interviews wherein the employee is probed for personal information by unauthorized or unscrupulous persons.

In addition, it is recommended that all personal information be kept in one place and informal or duplicate files be eliminated. Existing information that does not meet specified purposes or that is out of date should be destroyed or rendered anonymous.

10. Quality

To ensure the accuracy of personal information collected, Senior Concierge Providers policy is that individuals be given as much opportunity as reasonably possible

to review data files and update their information, particularly when it will be used for decision-making purposes.

11. Monitoring and Enforcement

Senior Concierge Providers policy is that the following procedures be implemented to address privacy-related inquiries and complaints:

- Logging-in: The date, time and nature of the complaint and the identity of the complainant should be recorded

- Acknowledgement: The organization should promptly acknowledge that the complaint is receiving attention.

- Decision: The decision as to how to handle the complaint should be based on appropriate legal requirements and the organization ' s privacy policies, made in a timely fashion, and consistent with previous decisions (a record of prior complaints and outcomes should be kept for this purpose).

- Response: A clear, prompt and helpful response should be communicated to the individuals. If the decision is adverse, the redress procedures should be made known to the individual. If it will take longer than 30 days to make the decision, the individual should be informed of the delay.

- Follow-up: The organization should contact the individual following the decision to verify whether the matter has been resolved in a satisfactory manner.

- Internal Review: A pattern of complaints in any one area should prompt the organizations compliance team to review its practices and procedures in that area.

In addition, the following procedures should be in place to deal with access requests from individuals:

- Making an official request: A request to review a personal information file should be made formally by asking in person and filling in a form, or by such means that would allow the organization to formally acknowledge and respond to the request.

- Verifying the identity of the individual: When a request for access to personal information files is made, the organization should require adequate identification of the individual making that request. If access requests are made by letter or over the telephone, means of establishing the identity of the individual seeking access must also be used. On a letter, the inclusion of customer identification numbers, mailing labels, drivers ' licenses or other similar types of identification along with the signature should be sufficient to establish identity.

12. Information not to be made available

- References to other individuals. For example, an employee file might contain references to the employee as a member of a task force or team.

Any comments about the other individuals on the team should not be provided to the employee seeking access to the file.

- Information that cannot be disclosed for legal or security reasons. If an individual was the subject of a security or legal investigation, release of any information pertaining to the investigation might jeopardize the outcome.

- Information that cannot be disclosed for commercial proprietary reasons. Examples of such information might include labor rates charged by companies for employees under contract, information used to establish ratings or eligibility or personal loans, insurance premiums or other information that, if disclosed, could be damaging to the commercial interests of an organization.

- Information that is subject to solicitor-client or litigation privilege.

- Information that cannot be disclosed for reasons of prohibitive cost. However, where the cost of access is considered to be too high, the individual should be given the opportunity to contribute to the cost, thereby reducing it.

- Establishing a time frame for response: Access requests should be dealt with promptly; a time frame of two weeks is suggested. If it will take longer than two weeks the individual making the request should be told how long they should expect to wait before receiving the information.

- The organization should keep a registry of access inquiries

- Updating or correcting information and withdrawing consent: If an individual requests that information be updated, corrected or deleted, or the consent for use be withdrawn, the organization should act on this request within a reasonable time (this period should not be longer that 30 days)

- Dispute resolution procedures: where the individual disputes the accuracy of the information held by the organization, the designated individual responsible to privacy compliance should review this issue. If the dispute is not settled to the satisfaction of the individual, the individual should be made aware of the existence of any industry associations or counsels, regulatory authorities or other agencies the individual can turn to for resolution of the dispute.

- Language and cultural issue: Reasonable efforts should be made to provide information in the format that the individual can readily understand.